تكوين مصادقة العامل الثنائي للجهاز للوصول إلى المطلب

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لتكوين مصادقة ثنائية العوامل باستخدام dot1x و مصادقة الجهاز.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين محرك خدمات الهوية من Cisco
- تكوين Cisco Catalyst
- المعيار IEEE802.1x

المكونات المستخدمة

- التصحيح 1 ل Identity Services Engine Virtual 3.3
- C1000-48FP-4G-L 15.2(7)E9

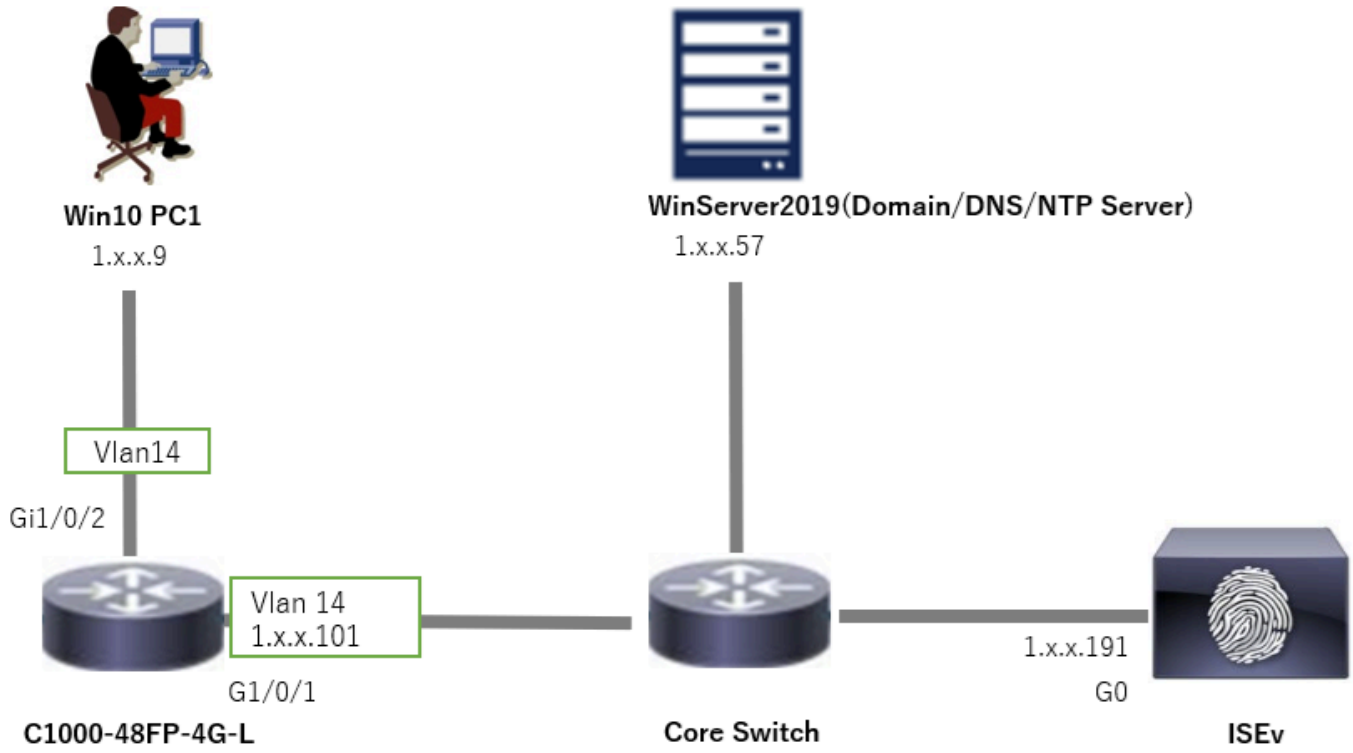
- نظام التشغيل Windows Server 2019

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الرسم التخطيطي للشبكة

تعرض هذه الصورة المخطط الذي يتم إستخدامه لمثال هذا المستند.

اسم المجال الذي تم تكوينه على Windows Server 2019 وهو ad.rem-xxx.com، والذي يتم إستخدامه كمثال في هذا المستند.



الرسم التخطيطي للشبكة

معلومات أساسية

مصادقة الجهاز هي عملية تأمين تتحقق من هوية الجهاز الذي يسعى للوصول إلى شبكة أو نظام. على عكس مصادقة المستخدم، التي تتحقق من هوية الشخص بناء على بيانات الاعتماد مثل اسم المستخدم وكلمة المرور، تركز مصادقة الجهاز على التحقق من صحة الجهاز نفسه. وغالبا ما يتم القيام بذلك باستخدام الشهادات الرقمية أو مفاتيح الأمان التي تكون فريدة للجهاز.

وباستخدام المصادقة الآلية ومصادقة المستخدم معا، يمكن للمؤسسة ضمان إمكانية الوصول إلى شبكتها من خلال الأجهزة والمستخدمين المعتمدين فقط، وبالتالي توفير بيئة أكثر أمانا. وتعد طريقة المصادقة ثنائية العوامل هذه مفيدة بشكل خاص لحماية المعلومات الحساسة والامتثال للمعايير التنظيمية الصارمة.

التكوينات

التكوين في C1000

هذا هو الحد الأدنى للتكوين في C1000 CLI.

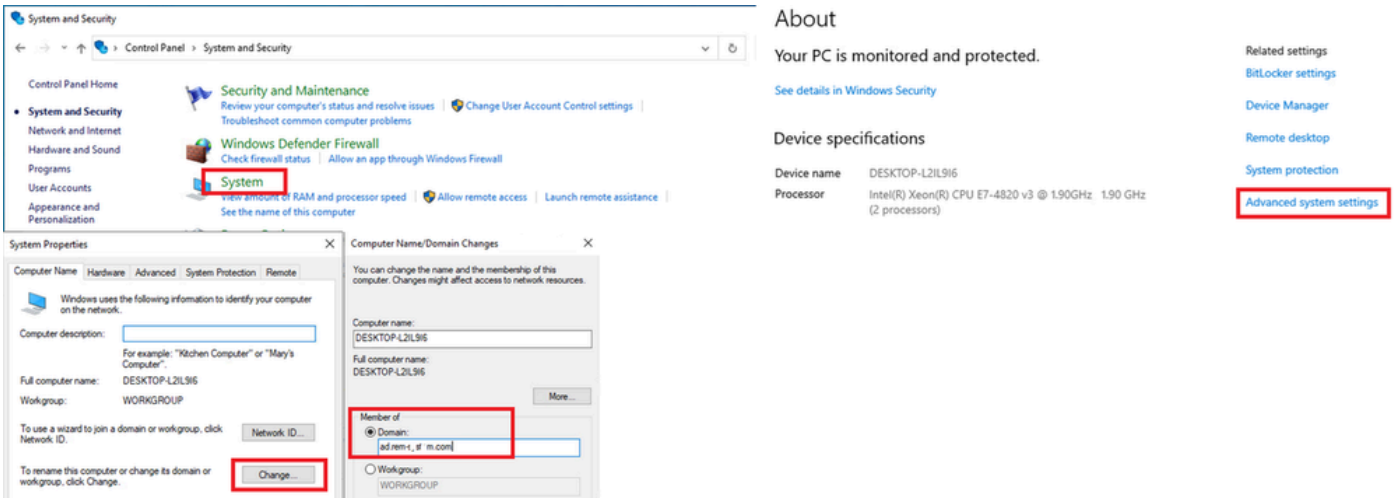
```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123
```

```
aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

التكوين في كمبيوتر Windows

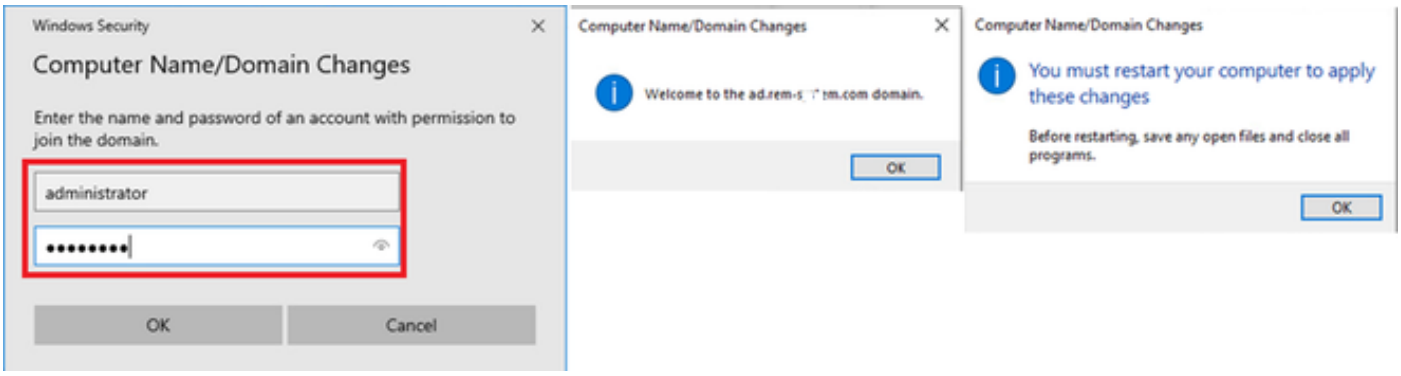
الخطوة 1. إضافة كمبيوتر إلى مجال AD

انتقل إلى لوحة التحكم > النظام والأمان، وانقر فوق النظام، ثم انقر فوق إعدادات النظام المتقدمة. في إطار "خصائص النظام"، انقر فوق تغيير، ثم حدد المجال وأدخل اسم المجال.



إضافة كمبيوتر إلى مجال AD

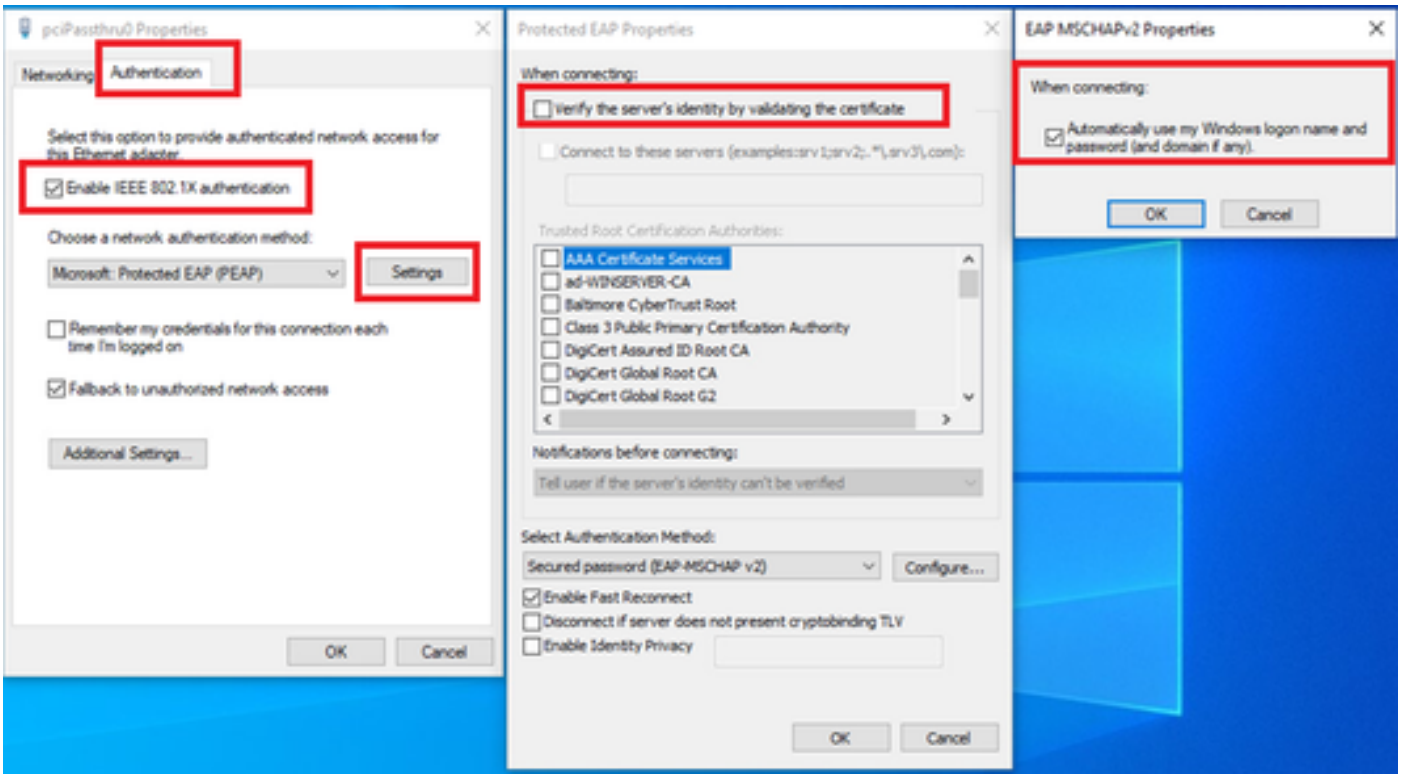
في نافذة "أمان Windows"، اسم مستخدم الإدخال وكلمة مرور خادم المجال.



إدخال اسم المستخدم وكلمة المرور

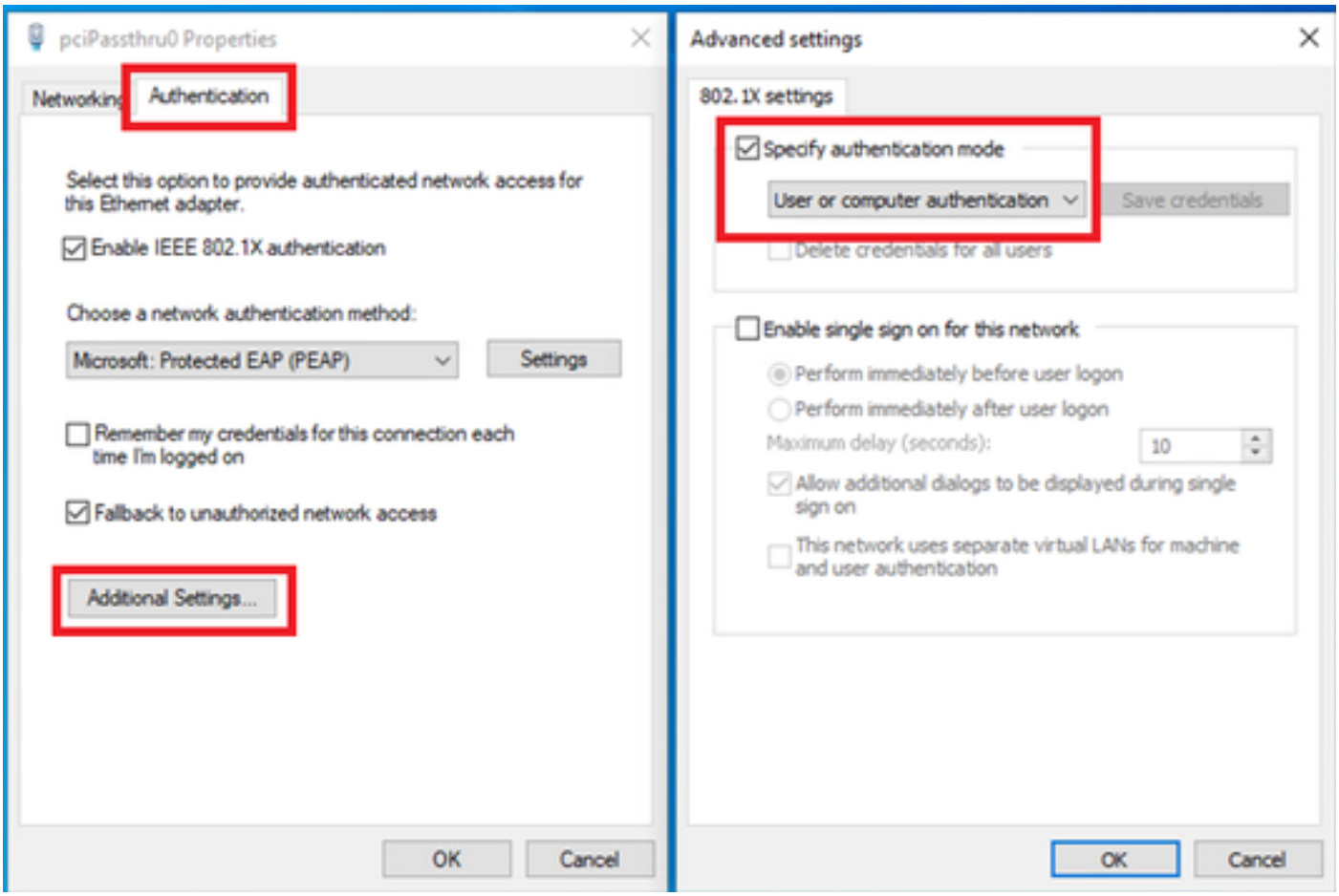
الخطوة 2. تكوين مصادقة المستخدم

انتقل إلى المصادقة، تحقق من تمكين مصادقة IEEE 802.1X. انقر على إعدادات في نافذة خصائص EAP المحمية، قم بإلغاء تحديد التحقق من هوية الخادم بالتحقق من صحة الشهادة ثم انقر على تكوين. في إطار خصائص EAP MSCHAPv2، تحقق من إستخدام اسم وكلمة مرور تسجيل الدخول إلى Windows تلقائيا (والمجال إن وجد) لاستخدام اسم المستخدم الذي تم إدخاله أثناء تسجيل دخول جهاز Windows لمصادقة المستخدم.



تمكين مصادقة المستخدم

انتقل إلى المصادقة، تحقق من الإعدادات الإضافية. حدد مصادقة المستخدم أو الكمبيوتر من القائمة المنسدلة.

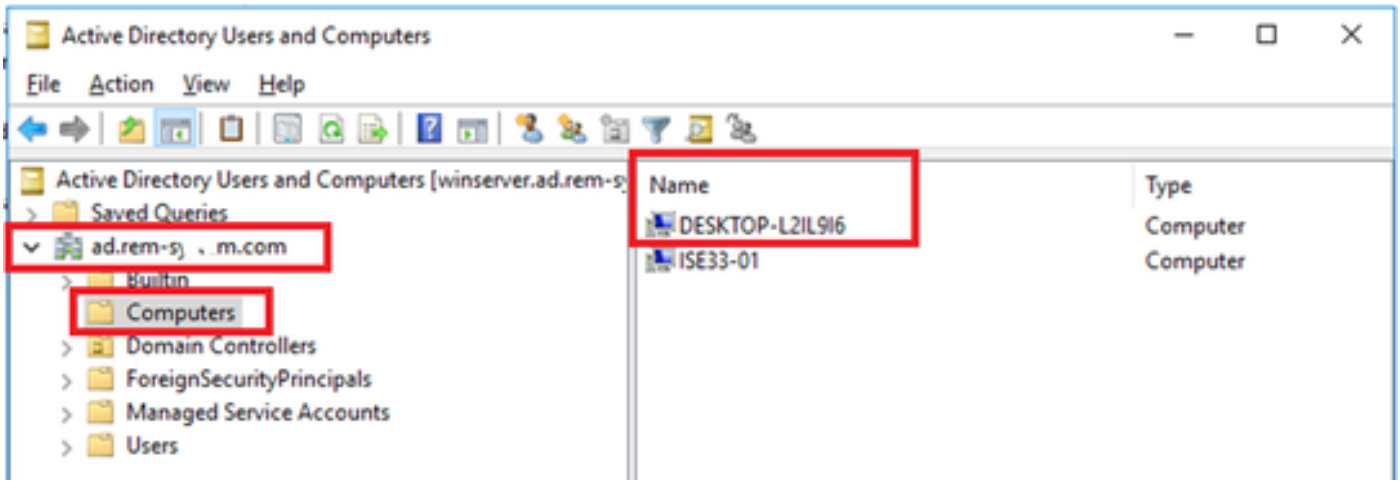


تحديد وضع المصادقة

التكوين في خادم Windows

الخطوة 1. تأكيد أجهزة كمبيوتر المجال

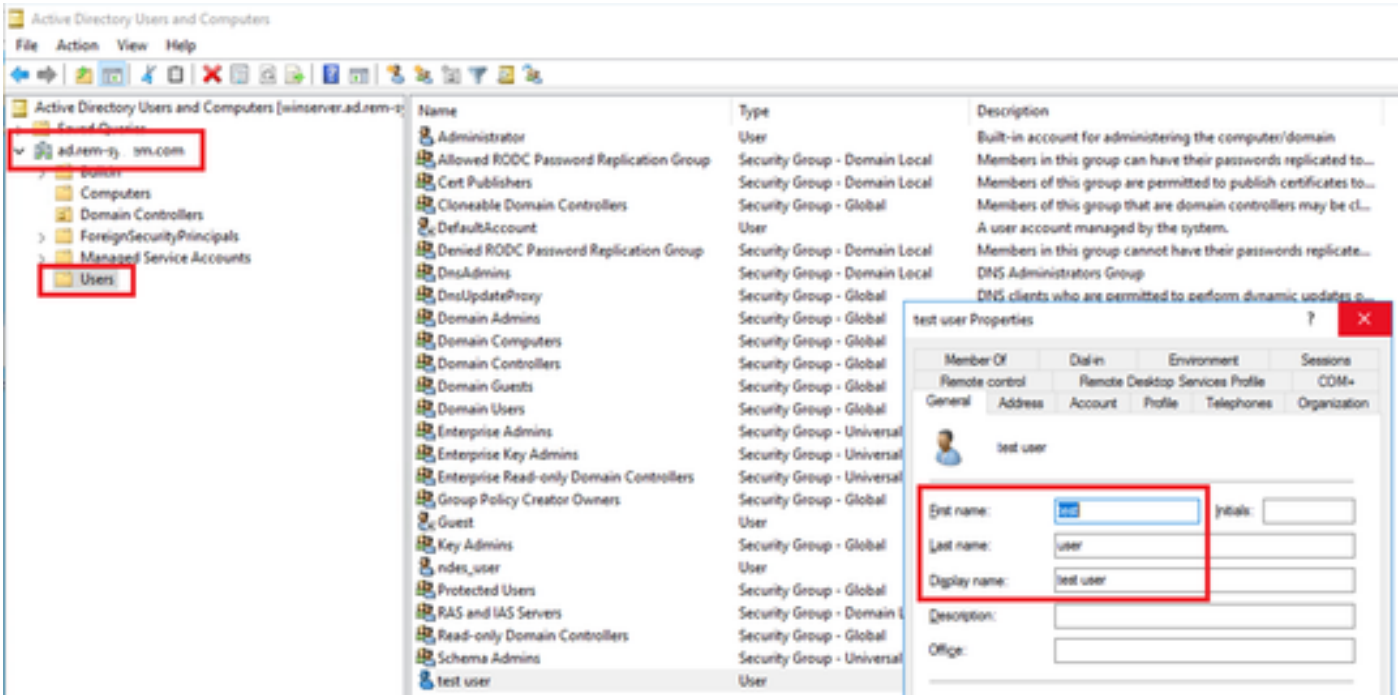
انتقل إلى مستخدمي Active Directory وأجهزة الكمبيوتر، انقر فوق أجهزة الكمبيوتر. تأكد من إدراج Win10 PC1 في المجال.



تأكيد كمبيوتر المجال

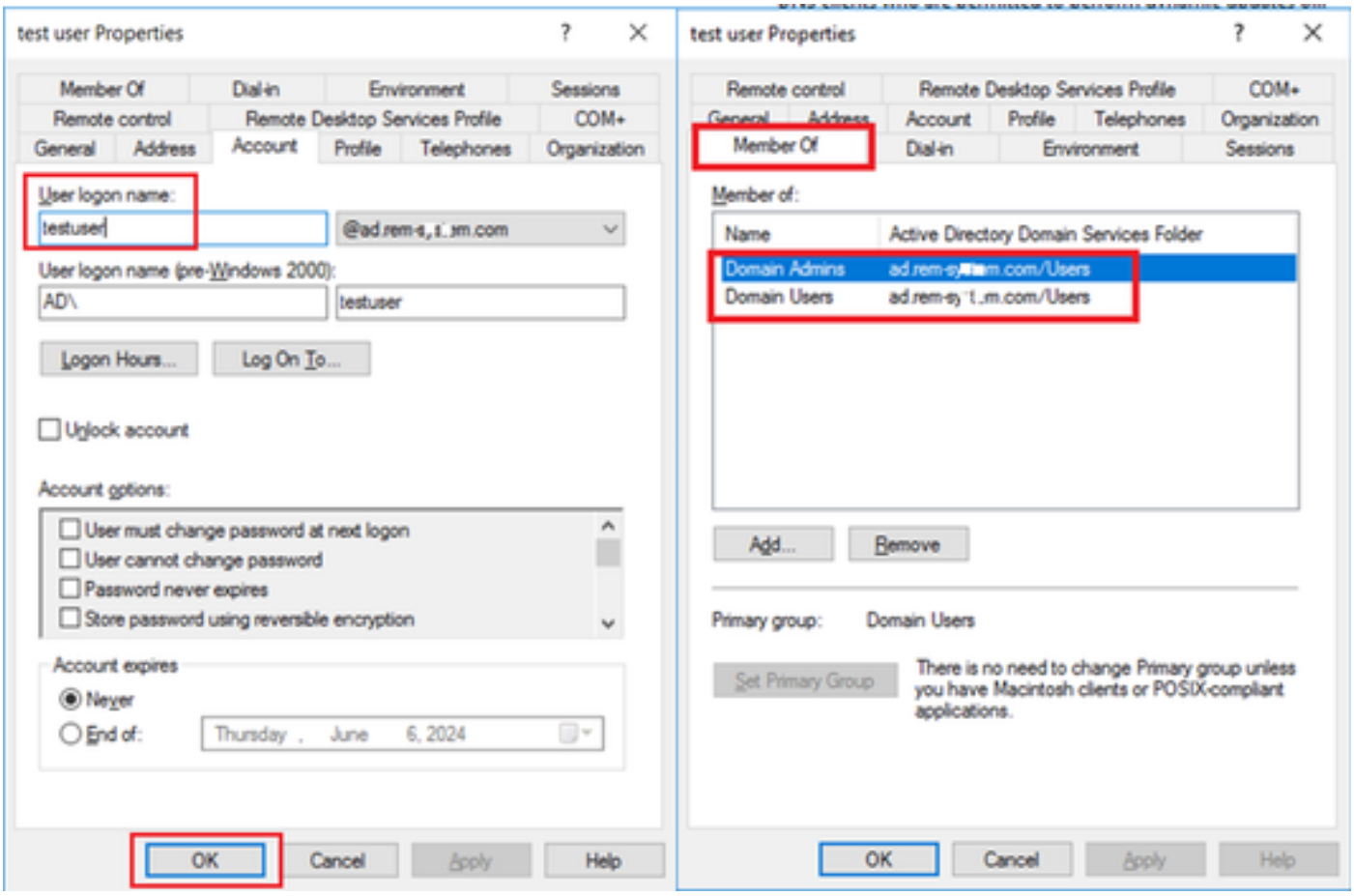
الخطوة 2. إضافة مستخدم مجال

انتقل إلى مستخدمي Active Directory وأجهزة الكمبيوتر، انقر فوق مستخدمين. إضافة مستخدم إختبار كمستخدم مجال.



إضافة مستخدم مجال

إضافة مستخدم المجال إلى عضو مسؤولي المجال ومستخدمي المجال.

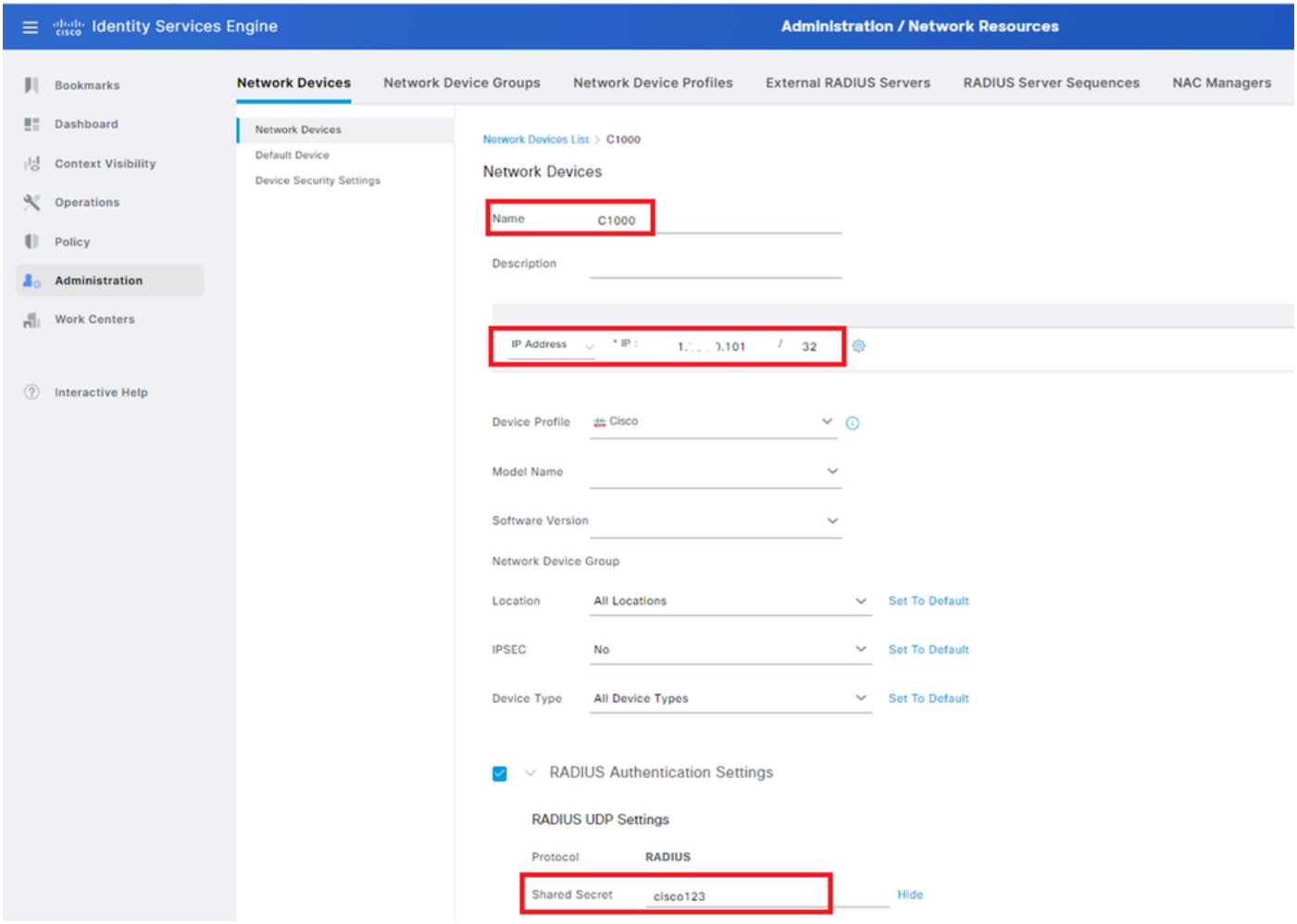


مسؤولو المجال ومستخدمو المجال

التكوين في ISE

الخطوة 1. إضافة جهاز

انتقل إلى إدارة > أجهزة الشبكة، انقر فوق إضافة زر لإضافة جهاز C1000.

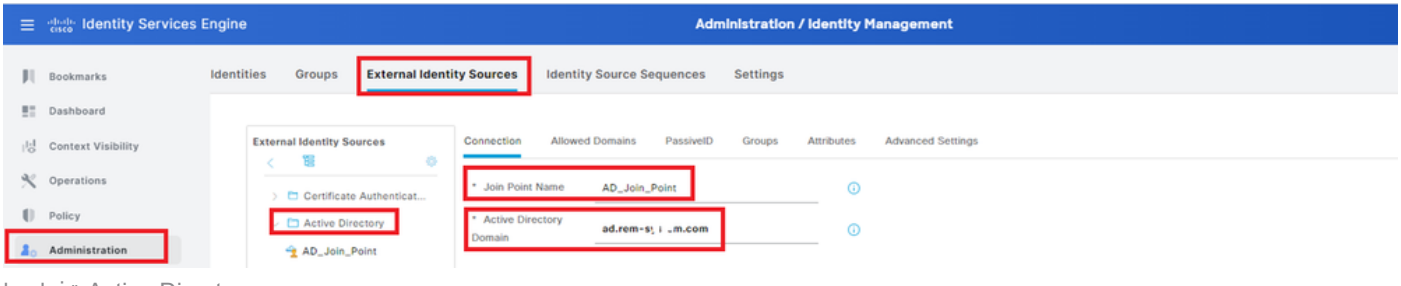


إضافة جهاز

الخطوة 2. إضافة Active Directory

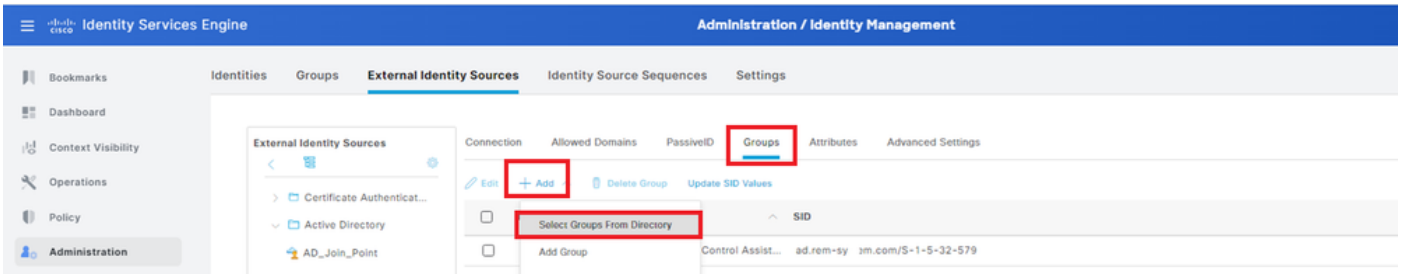
انتقل إلى إدارة > مصادر الهوية الخارجية > Active Directory، وانقر فوق علامة التبويب اتصال، وقم بإضافة Active Directory إلى ISE.

- اسم نقطة الربط: AD_JOIN_POINT
- مجال خدمة Active Directory: ad.rem-xxx.com



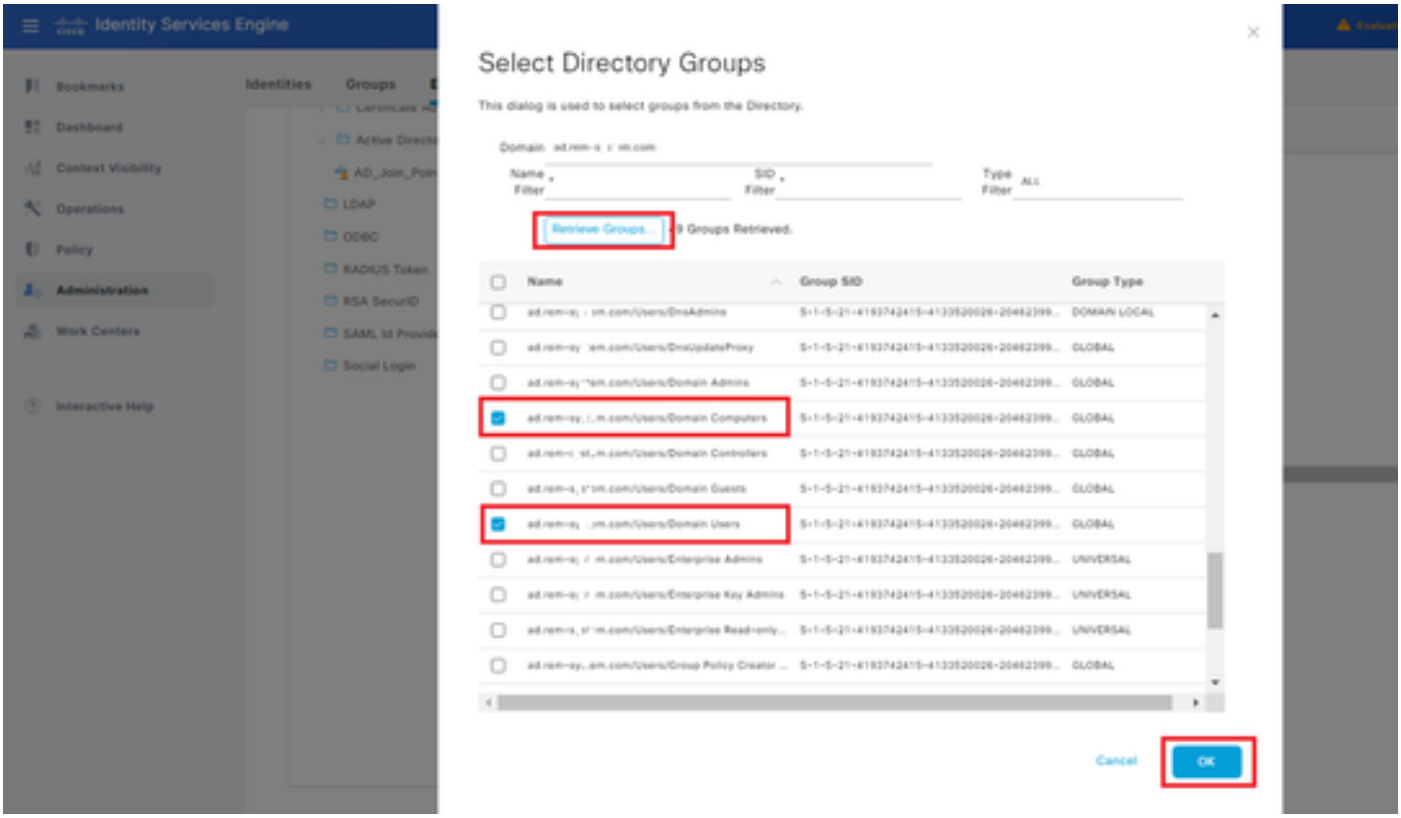
إضافة Active Directory

انتقل إلى علامة التبويب مجموعات، حدد تحديد مجموعات من الدليل من القائمة المنسدلة.



تحديد مجموعات من الدليل

انقر فوق إسترداد المجموعات من القائمة المنسدلة. تحقق من أجهزة الكمبيوتر على العنوان ad.rem-xxx.com/Users/Domain ومستخدمي ad.rem-xxx.com/Users/Domain وانقر فوق موافق.



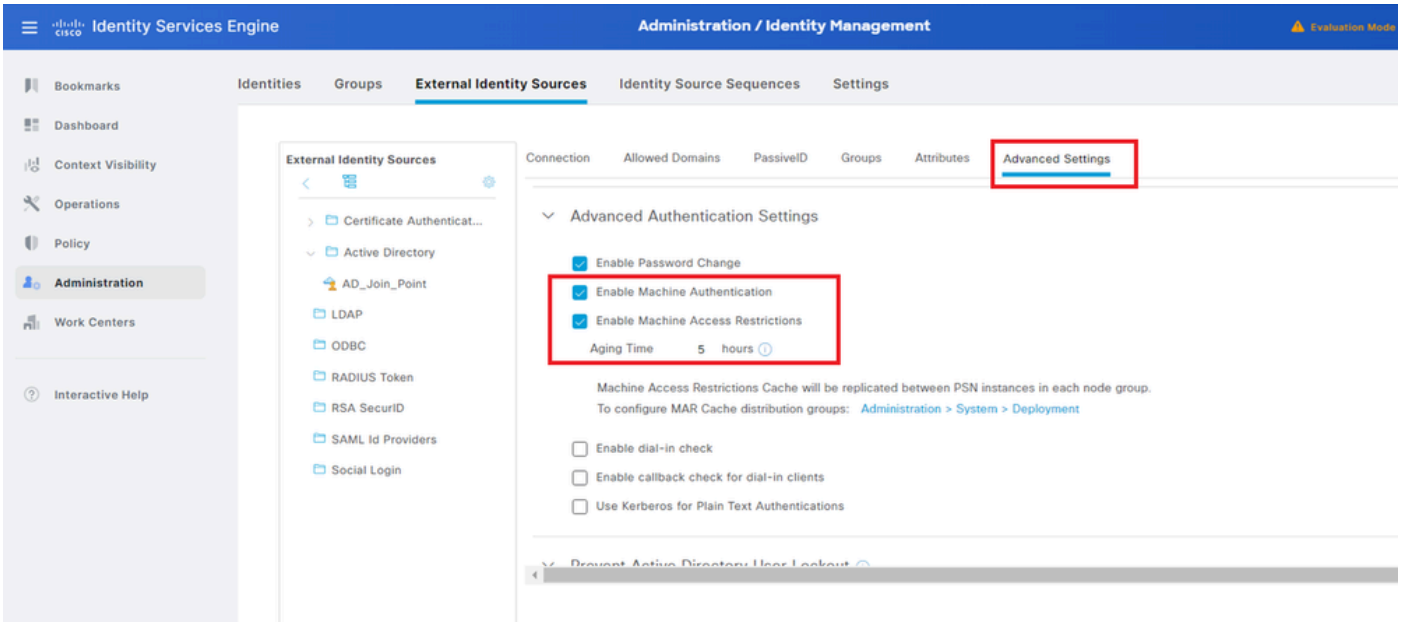
إضافة أجهزة كمبيوتر المجال والمستخدمين

الخطوة 3. تأكيد إعداد مصادقة الجهاز

انتقل إلى علامة التبويب إعدادات متقدمة، وتأكد من إعداد مصادقة الجهاز.

- تمكين مصادقة الجهاز: لتمكين مصادقة الجهاز
- تمكين "قيد الوصول إلى الجهاز": لدمج مصادقة المستخدم والآلة قبل التخويل

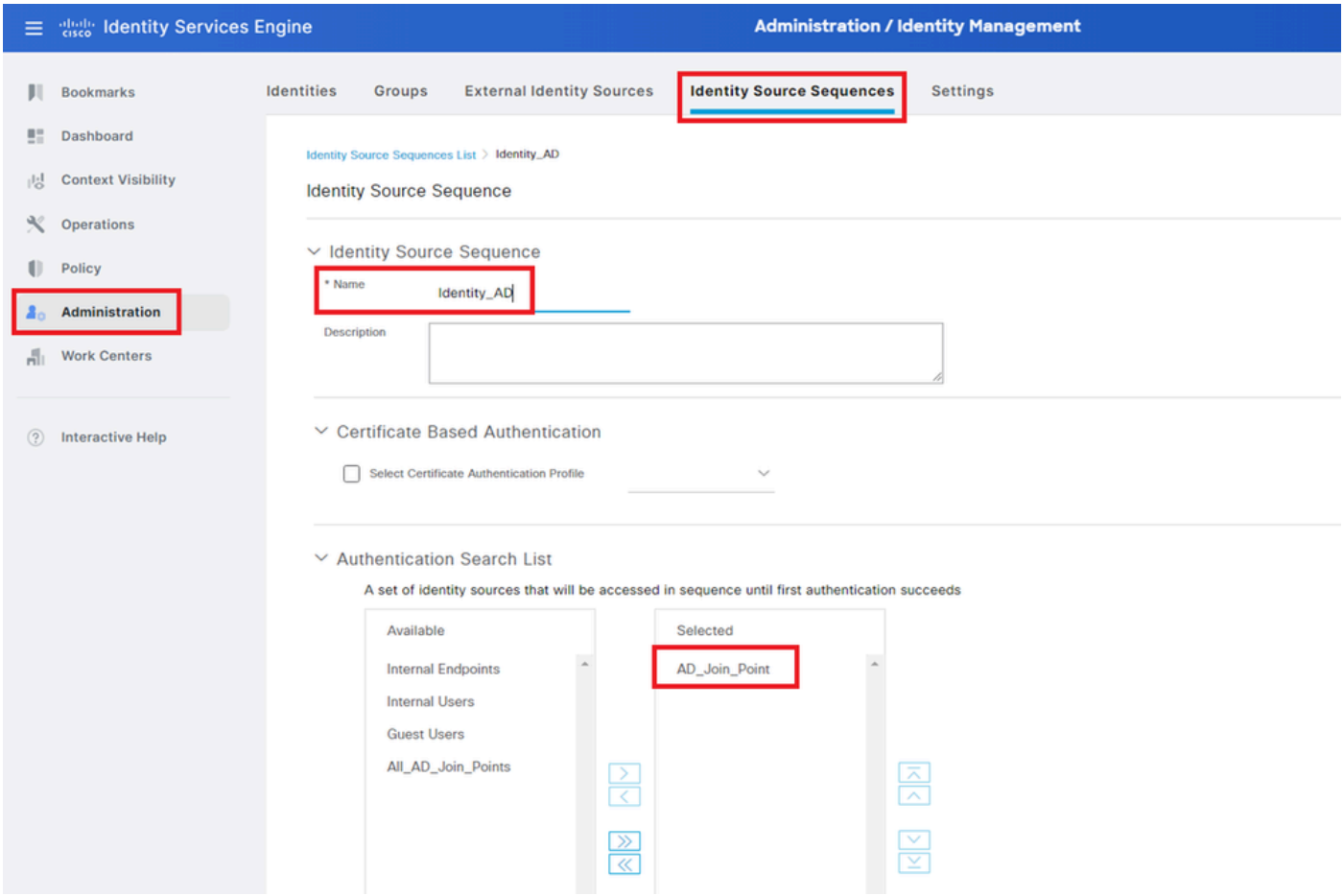
ملاحظة: النطاق الصحيح لوقت التقادم هو من 1 إلى 8760.



الخطوة 4. إضافة تسلسلات مصدر الهوية

انتقل إلى إدارة > تسلسلات مصدر الهوية، وقم بإضافة تسلسل مصدر هوية.

- الاسم: Identity_AD
- قائمة البحث عن المصادقة: AD_JOIN_POINT

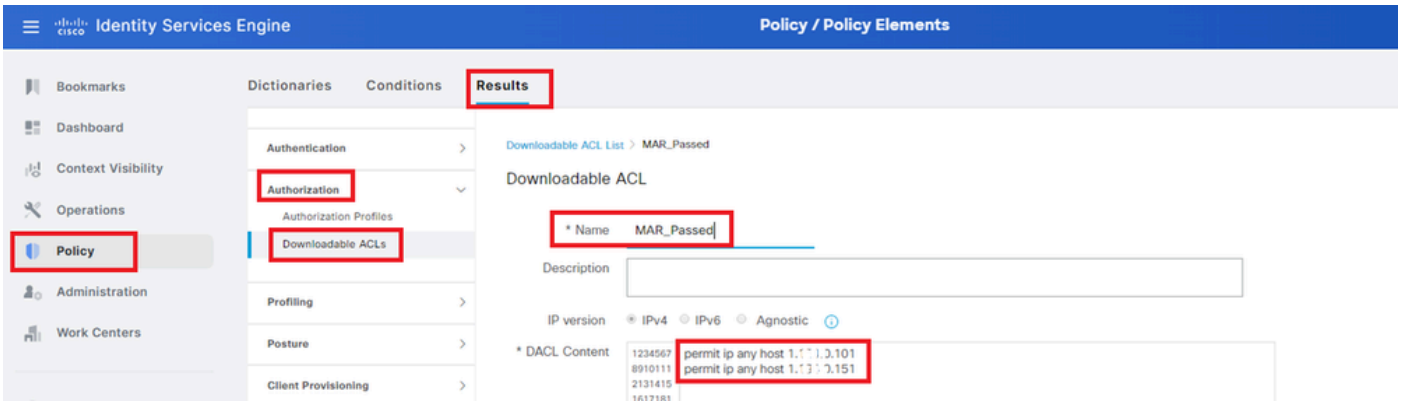


إضافة تسلسلات مصدر الهوية

الخطوة 5. إضافة DACL وملف تعريف التخويل

انتقل إلى السياسة > النتائج > التفويض > قوائم التحكم في الوصول (ACL) القابلة للتنزيل، وقم بإضافة قائمة التحكم في الوصول (DACL).

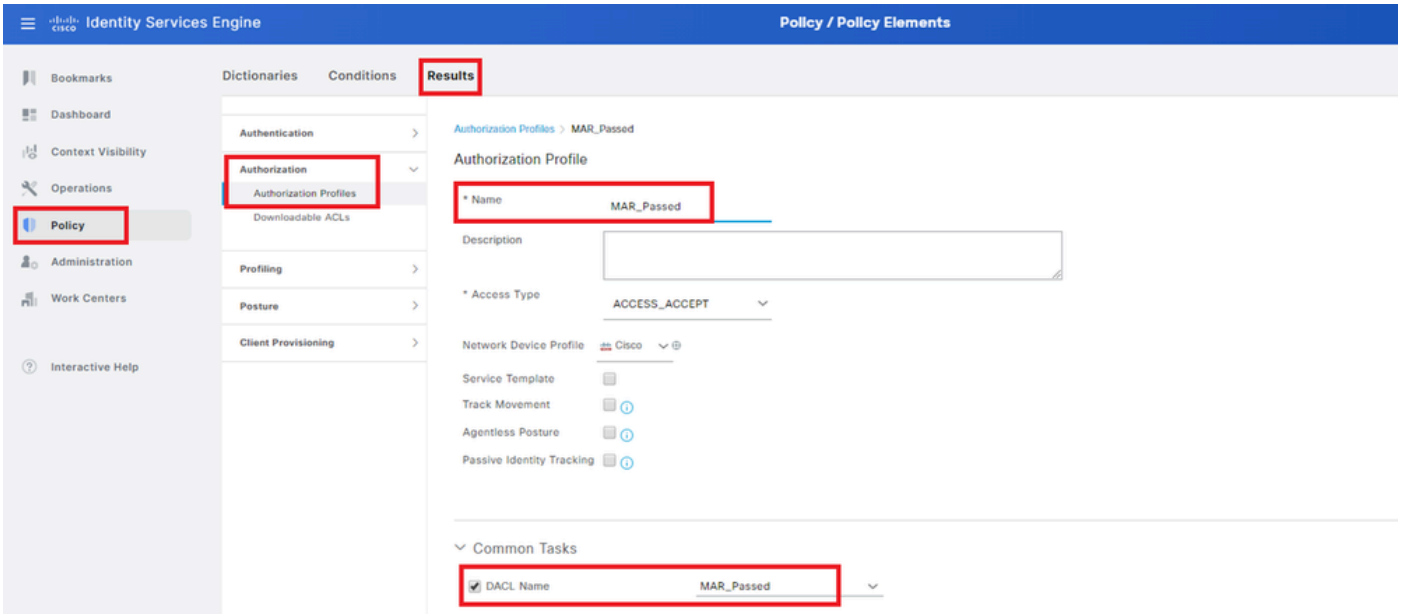
- الاسم: MAR_PASS
- محتوى قائمة التحكم في الوصول إلى البنية الأساسية (DACL): السماح لـ IP بأي مضيف 1.x.x.101 والسماح لـ IP أي مضيف 1.x.105



إضافة DACL

انتقل إلى السياسة > النتائج > التخويل > توصيفات التخويل، وأضف ملف تعريف تخويل.

- الاسم: MAR_PASS
- اسم DACL: MAR_PASS

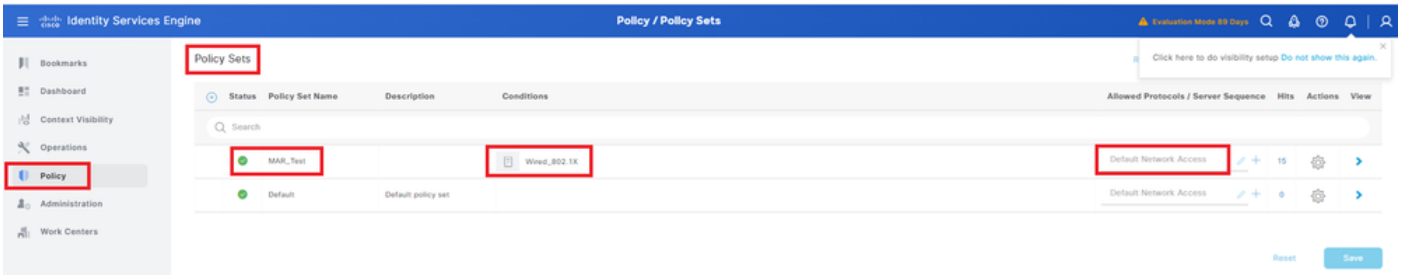


إضافة ملف تعريف التخويل

الخطوة 6. إضافة مجموعة نمج

انتقل إلى نمج > مجموعات نمج، انقر فوق + لإضافة مجموعة نمج.

- اسم مجموعة النمج: MAR_TEST
- الشروط: WIRED_802.1X
- البروتوكولات المسموح بها / تسلسل الخادم: الوصول الافتراضي إلى الشبكة

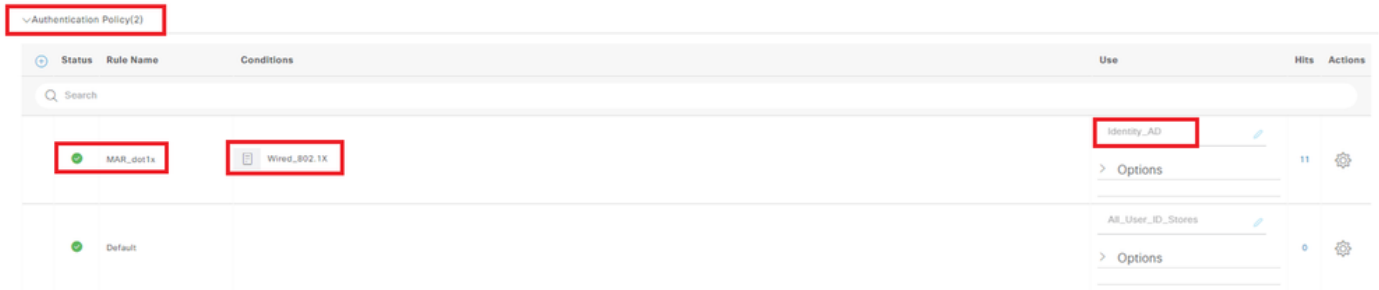


إضافة مجموعة نهج

الخطوة 7. إضافة نهج المصادقة

انتقل إلى مجموعات النهج، انقر فوق MAR_TEST لإضافة نهج مصادقة.

- اسم القاعدة: MAR_DOT1x
- الشروط: WIRED_802.1X
- الاستخدام: Identity_AD



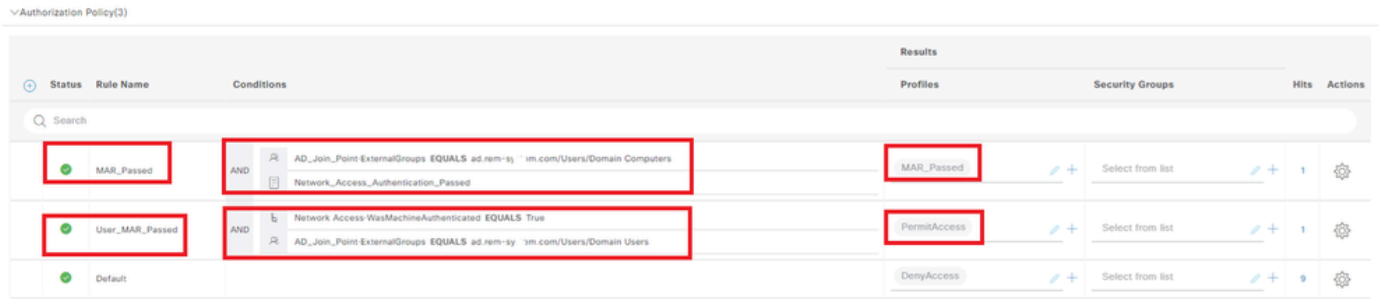
إضافة نهج المصادقة

الخطوة 8. إضافة نهج التخويل

انتقل إلى مجموعات النهج، وانقر فوق MAR_TEST لإضافة نهج تخويل.

- اسم القاعدة: MAR_PASS
- الشروط: تساوي AD_JOIN_POINT·ExternalGroups ad.rem-xxx.com/Users/Domain Computers وNetwork_ACCESS_AUTHENTICATION_PASS
- النتائج: MAR_PASS

- اسم القاعدة: user_mar_pass
- الشروط: Network Access·WasMachineAuthenticated يساوي True وAD_JOIN_Point·ExternalGroups يساوي مستخدمي ad.rem-xxx.com/Users/Domain
- النتائج: PermitAccess



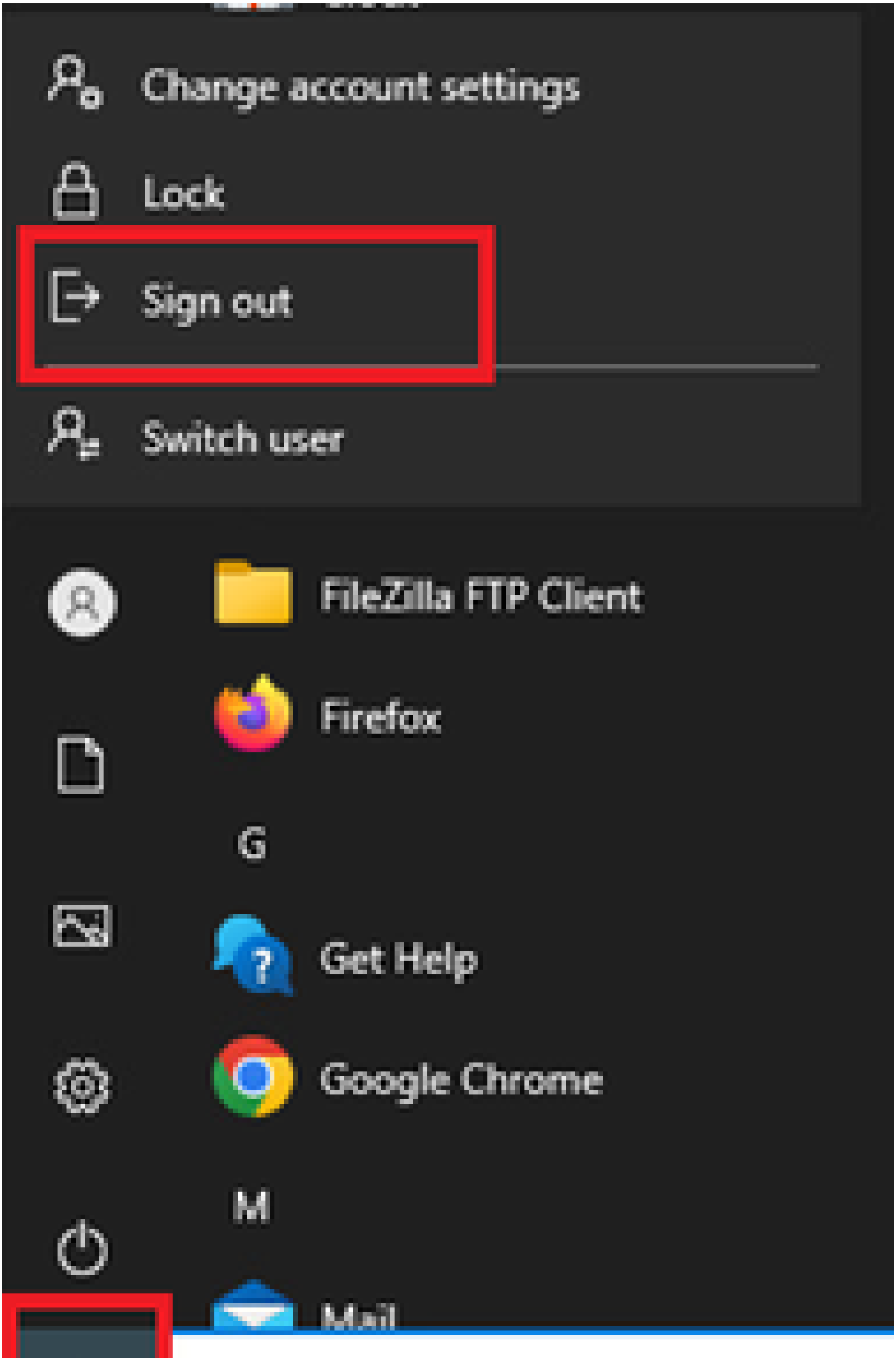
إضافة نهج التخويل

التحقق من الصحة

النمط 1. مصادقة الجهاز ومصادقة المستخدم

الخطوة 1. تسجيل الخروج من Windows PC

انقر فوق زر تسجيل الخروج من Win10 PC1 لتشغيل مصادقة الجهاز.


Change account settings
Lock
Sign out
Switch user
FileZilla FTP Client
Firefox
G
Get Help
Google Chrome
M
Mail

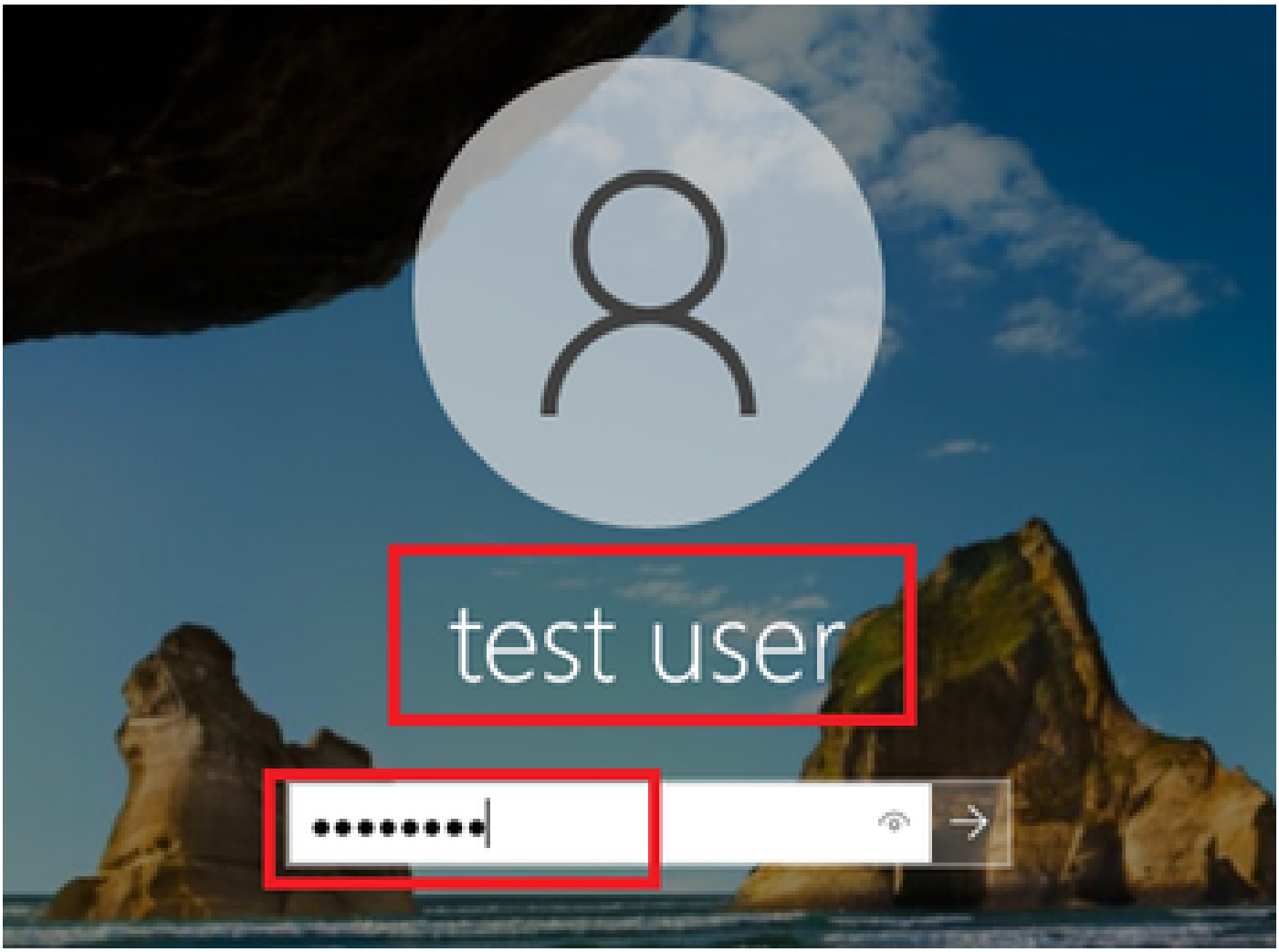
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 5s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003C
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success
```

الخطوة 3. تسجيل دخول Windows PC

قم بتسجيل الدخول إلى Win10 PC1 واسم مستخدم الإدخال وكلمة مرور لتشغيل مصادقة المستخدم.



تسجيل دخول *Windows PC*

الخطوة 4. تأكيد جلسة عمل المصادقة

قم بتشغيل show authentication sessions interface GigabitEthernet1/0/2 details الأمر لتأكيد جلسة مصادقة المستخدم في C1000.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

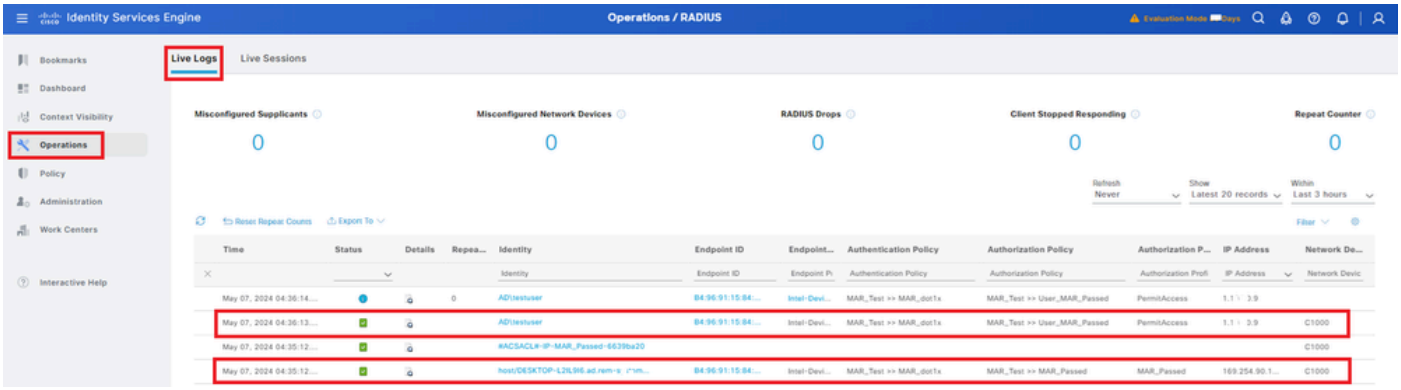
AD\testuser

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
```

```
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

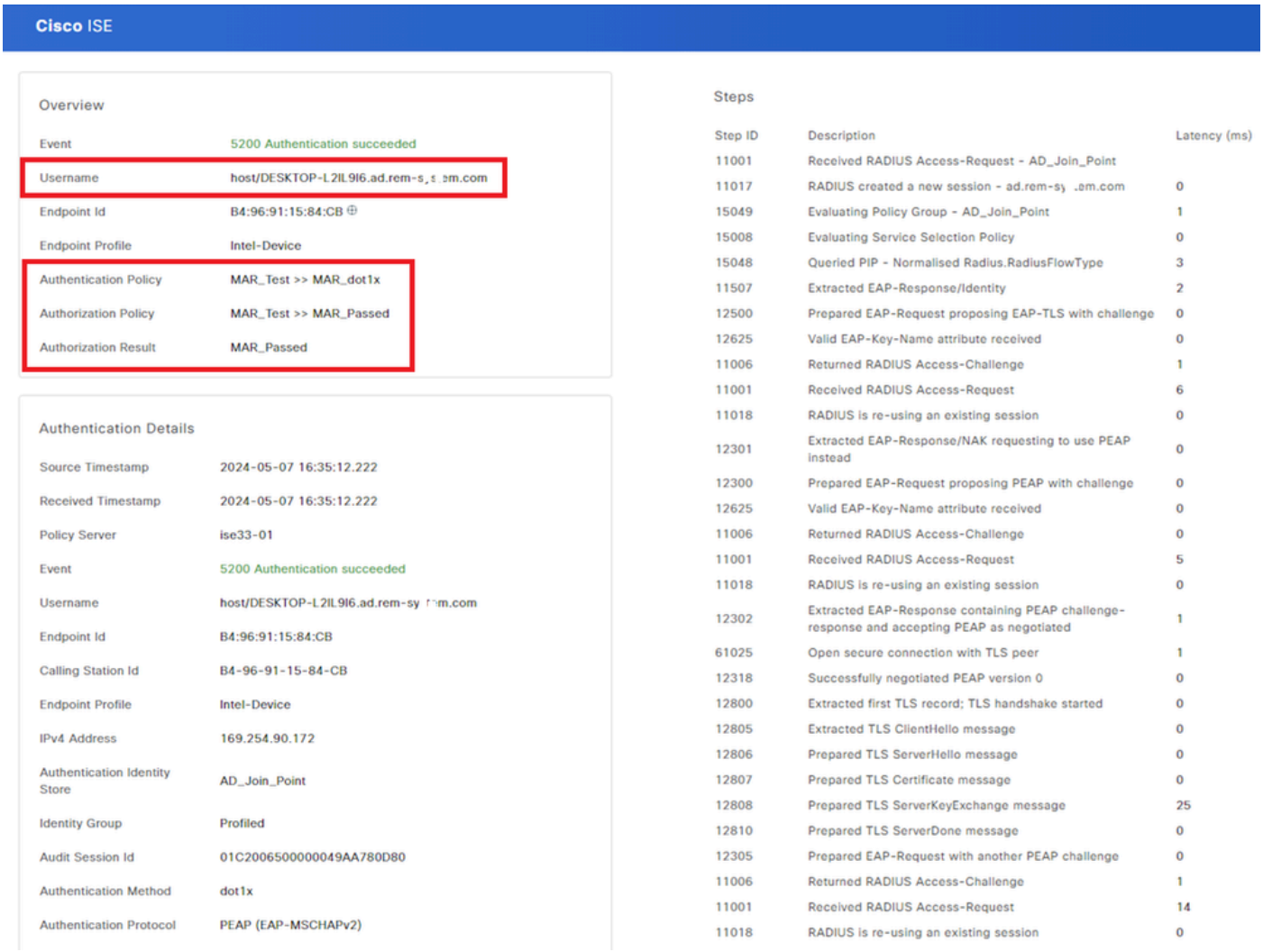
الخطوة 5. تأكيد سجل Radius Live

انتقل إلى **العمليات > RADIUS > السجلات المباشرة** في واجهة المستخدم الرسومية (ISE)، وتأكد من سجل التشغيل لمصادقة الجهاز ومصادقة المستخدم.



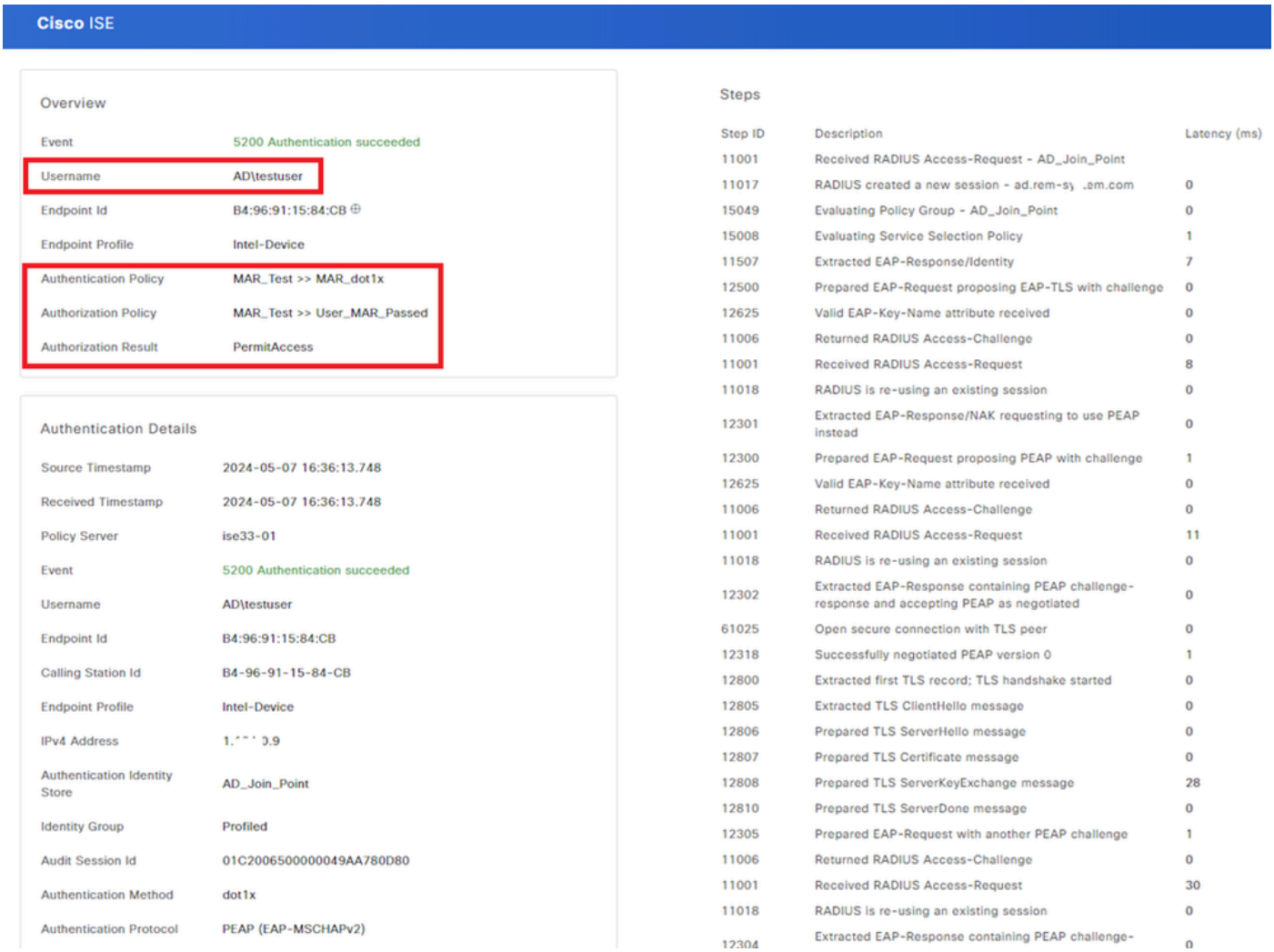
سجل *Radius Live*

تأكيد سجل التشغيل التفصيلي لمصادقة الجهاز.



تفاصيل مصادقة الجهاز

قم بتأكيد السجل المباشر المفصل لمصادقة المستخدم.



تفاصيل مصادقة المستخدم

النمط 2. مصادقة المستخدم فقط

الخطوة 1. تعطيل وتمكين NIC من Windows PC

لتشغيل مصادقة المستخدم، قم بتعطيل وتمكين بطاقة واجهة الشبكة (NIC) الخاصة ب Win10 PC1.

الخطوة 2. تأكيد جلسة عمل المصادقة

قم بتشغيل show authentication sessions interface GigabitEthernet1/0/2 details الأمر لتأكيد جلسة مصادقة المستخدم في C1000.

<#root>

Switch#

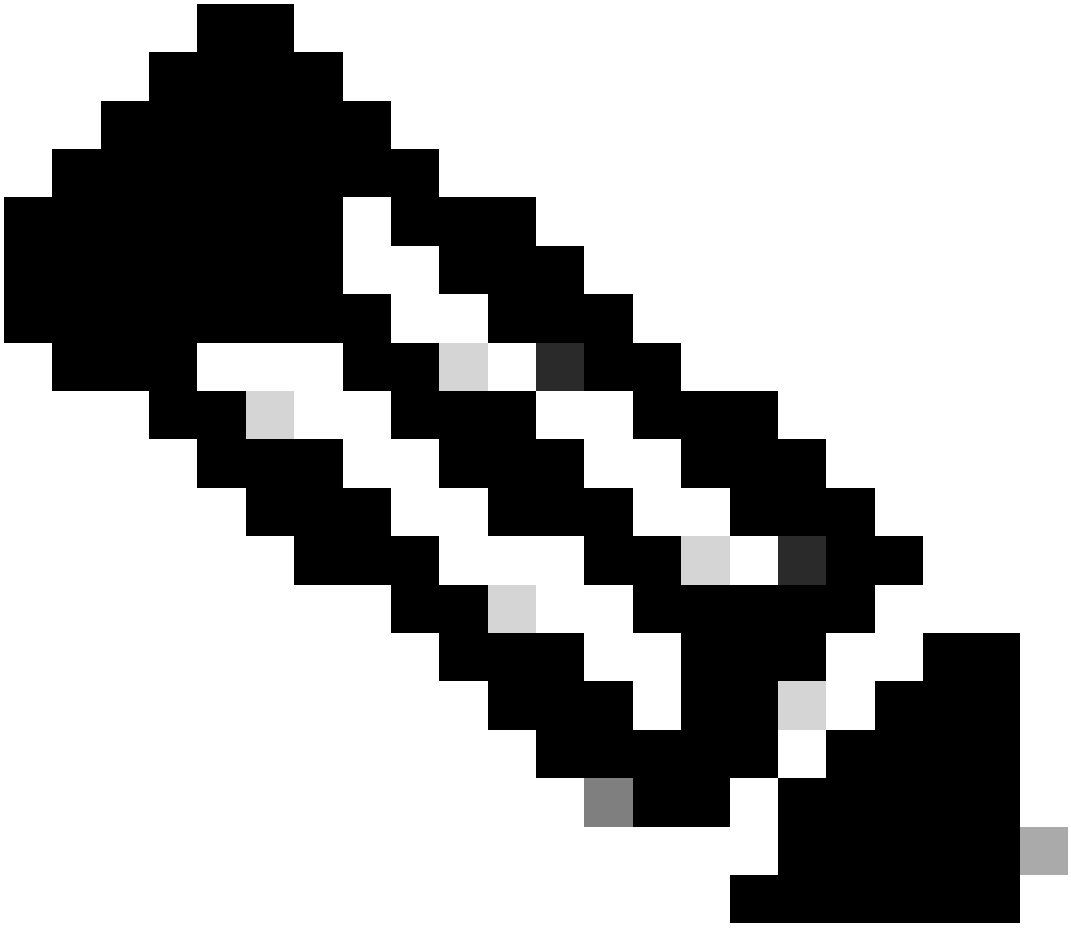
show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name: AD\testuser
```

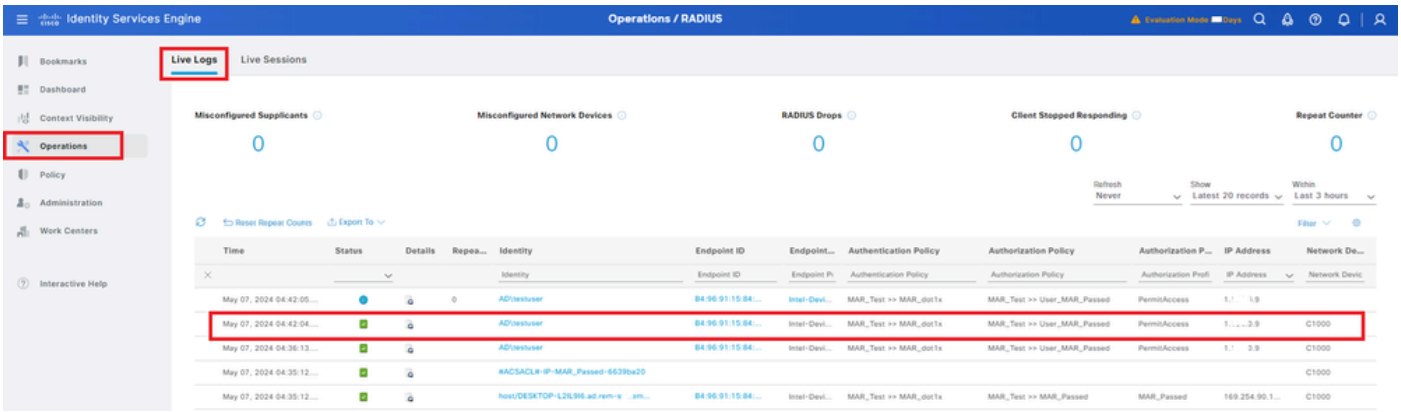
```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

الخطوة 3. تأكيد سجل Radius Live

انتقل إلى العمليات > **RADIUS** > السجلات المباشرة في واجهة المستخدم الرسومية (ISE)، وقم بتأكيد السجل النشط لمصادقة المستخدم.

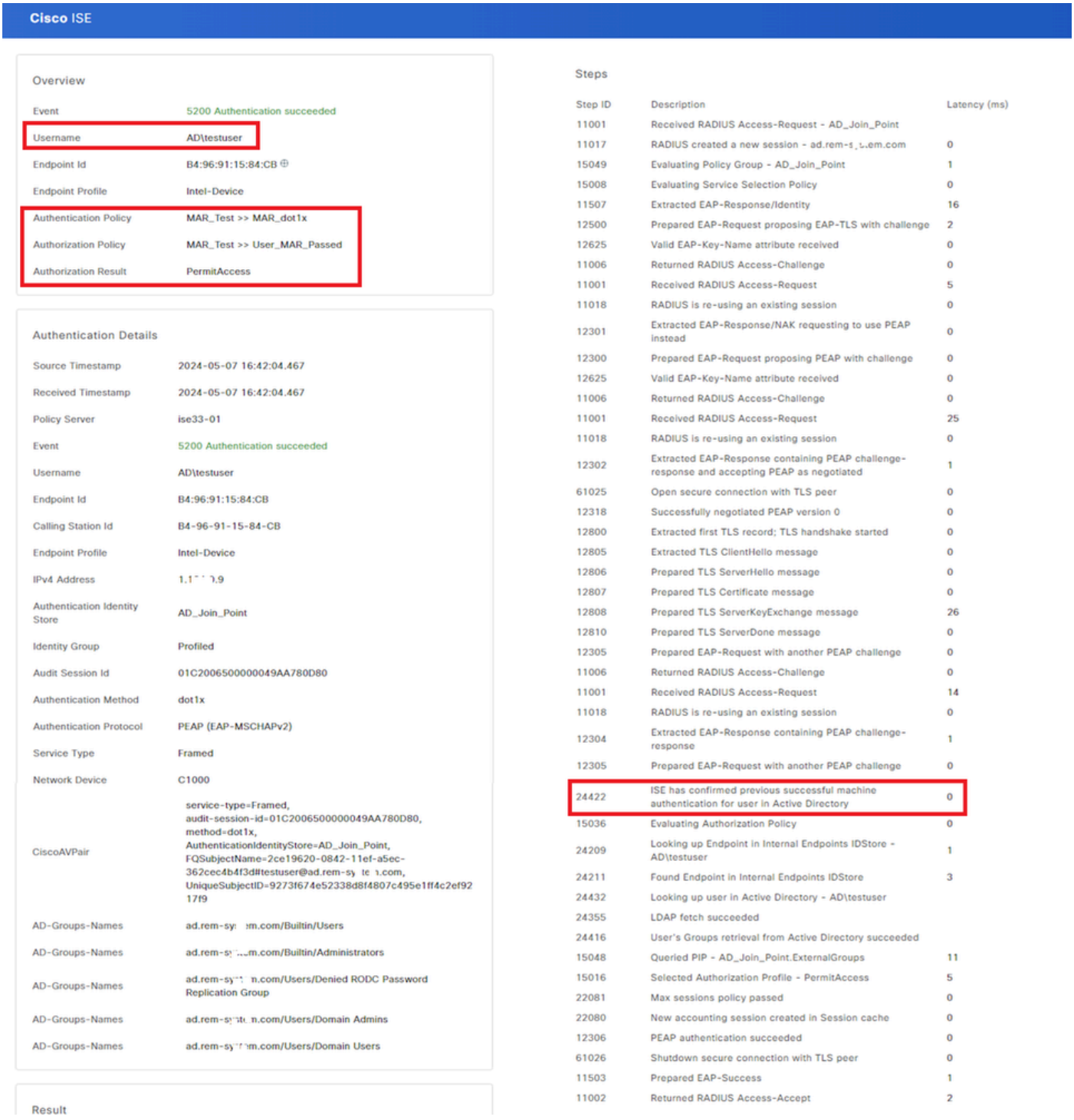


ملاحظة: نظرا لأنه يتم تخزين ذاكرة التخزين المؤقت ل MAR في ISE، يلزم فقط مصادقة المستخدم.



سجل *Radius Live*

قم بتأكيد السجل المباشر المفصل لمصادقة المستخدم.



تفاصيل مصادقة المستخدم

استكشاف الأخطاء وإصلاحها

تساعدك سجلات تصحيح الأخطاء هذه (prrt-server.log) على تأكيد السلوك التفصيلي للمصادقة في ISE.

- runtime-config

- تسجيل وقت التشغيل
- Runtime-AAA

هذا مثال على سجل تصحيح الأخطاء للنمط **1.** مصادقة الجهاز ومصادقة المستخدم في هذا المستند.

<#root>

// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com, IDStore=AD_Join_Point an
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222
MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

معلومات ذات صلة

[الإجراءات والسلاسل الخاصة بتقييد الوصول إلى الجهاز](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).